Prospect Theory and Information Security Investment Decisions

Diana Young
Information Systems, University of Texas at San Antonio, San Antonio, TX, United States., Diana.young@utsa.edu

Nicole Beebe
Information Systems & Technology Management, The University of Texas at San Antonio, San Antonio, TX, United States., nicole.beebe@utsa.edu

Frederick Chang
Information Systems & Technology Management, The University of Texas at San Antonio, San Antonio, TX, United States., fred.chang@utsa.edu

Prospect Theory and Information Security Investment Decisions

Diana K. Young
University of Texas at San Antonio
diana.young@utsa.edu

Nicole L. Beebe
University of Texas at San Antonio
nicole.beebe@utsa.edu

Frederick R. Chang
University of Texas at San Antonio
fred.chang@utsa.edu

ABSTRACT

Most articles that discuss the economics of security focus on the use of rational choice decision models for evaluating investment alternatives. However, security investment decisions involve risk and several researchers have noted that risk related decisions often violate the fundamental principles of rational choice decision models. Accordingly, we assert that problems exist with using these models to explain security investment decisions. Further, we believe that the development of prescriptive models to guide investment decisions requires a deeper understanding of the cognitive processes involved. To test these ideas, we introduce a study that uses prospect theory to analyze security practitioners' investment decisions. The article includes a discussion of our methodology to electronically assess security practitioners' preference patterns. Additionally, we discuss data collection efforts which are currently in-process and future plans to analyze the collected data. Interim analytical results of data received prior to AMCIS 2012 will be presented to conference attendees.

Keywords

information security, security economics, security management, prospect theory, decision theory

INTRODUCTION

The need for more research concerning information security investments has been noted in the literature (Computing Researcher Association 2006; U.S. Department of Homeland Security 2009; Zafar and Clark 2009). While a hand-full of articles addressing the topic have been published, the majority focus on the use of rational choice decision models to evaluate investment alternatives (Cavusoglu, Cavusoglu and Raghunathan 2004a; Cavusoglu, Mishra and Raghunathan 2004b; Cavusoglu, Raghunathan and Yue 2008; Gal-Or and Ghose 2005; Gordon and Loeb 2002; Herath and Herath 2008). Rational choice models are premised on the assumptions that decision makers: 1) calculate the value of choice alternatives using stated probabilities and outcomes, 2) apply probabilities linearly as decision weights, and 3) choose alternatives that yield the highest net value (Crozier and Ranyard 1997).

While research based on rational choice models provides normative guidance concerning investment options, it is important to note two key problems with applying these models to the information security investment context. First, rational choice models theorize that individuals calculate the value of each alternative using known probabilities and outcomes. However, the probability of occurrence and financial consequences resulting from security events are rarely known a priori. Further, accurate estimation of these values is widely recognized as a highly challenging endeavor for even the most experienced practitioner (Computing Researcher Association 2006; U.S. Department of Homeland Security 2009). The second problem with applying rational choice models in the security context concerns the postulation that individuals apply probabilities linearly as decision weights. IS security investment decisions are risk related, and several researchers have

noted that risk related decisions are often characterized by phenomena which violate the fundamental principles of rational choice decision models. These phenomena include: 1) nonlinear application of probabilities as decision weights, 2) different risk attitudes toward gains and losses, and 3) preferences for certain outcomes over merely probabilistic outcomes (Allais 1953; Crozier and Ranyard 1997; Kahneman and Tversky 1979; Slovic, Fischhoff and Lichtenstein 1977; Tversky and Kahneman 1992).

To explain these pervasive inconsistencies with rational choice models, Kahneman and Tversky (1979) proposed prospect theory which they later defined as the "approximate, incomplete, simplified description of the evaluation of risky prospects." Central to prospect theory is the concept of framing. Tversky and Kahneman defined framing as the manner in which a statement or question is worded, such that the wording influences the "decision maker's conception of the acts, contingencies, and outcomes" of the given options (1981, p. 453). During the course of their studies, Tversky and Kahneman found that individuals exhibit significantly different preference patterns when choosing between options framed as gains and options framed as loses. Prospect theory is considered the most influential of all descriptive decision theories (Crozier and Ranyard 1997) and has been used to study risk related decisions in a variety of disciplines (Church, Libby and Ping 2008; Devers, McNamara, Wiseman and Arrfelt 2008; Edwards, Miles Jr. and Von Winterfeld 2007; Latham and Braun 2009; Wagner, Hennig-Thurau and Rudolph 2009). The notion of using prospect theory to explain users' information security related behavior was suggested by West (2008) but was not empirically tested.

The purpose of this study is to determine if prospect theory informs information security investment decisions. Specifically, we investigate whether or not the framing of choice options influences security professionals' investment decisions. The findings of this study will add to our current understanding of the factors that bias security practitioner's perceptions of investment options and lead them to make non-rational decisions. Prior decision theory research (Edwards et al. 2007), has shown that a keen awareness of these factors when applying normative decision models can enhance an individual's ability to make a rational decision. For academics, this study contributes by providing descriptive, behavioral information that helps explain information security investment decisions. For practitioners, this study contributes by acquiring key information needed toward the development of decision aids and decision models. Both areas have received little research attention to date.

The remainder of the paper is structured as follows. The next section provides a review of the literature surrounding the topics of IS security investment, decision theory, and prospect theory. Following the articulation of our research hypothesis, we explain our methodology to assess security practitioners' choice patterns when faced with hypothetical security investment decisions. Following the methodology section we present our data collection plan, proposed data analysis method, and concluding remarks.

LITERATURE REVIEW

IS Security Investment

Interest in IS security research has increased dramatically since the early 1990s (Zafar and Clark 2009). While the majority of the literature produced to date focus on security governance, data integrity, privacy, and threat mitigation issues, a few authors have concentrated their efforts on the economic implications of security (Cavusoglu et al. 2004a; Cavusoglu et al. 2004b; Cavusoglu et al. 2008; Gal-Or and Ghose 2005; Gordon and Loeb 2002; Herath and Herath 2008; Zafar and Clark 2009). Using normative decision theory as a guide, Gordon and Loeb (2002) proposed an economic model to help determine the optimal security investment level. Their proposed model derives the expected utility of security investment options by comparing the probabilistic benefits accrued from investments to their associated costs. When testing the model via computer simulation, the researchers found that economic justification is only appropriate for investments characterized by moderate levels of system vulnerability - security investments in systems with very low or extremely high levels of vulnerability could not be justified economically using the model. Further, they concluded that a firm's maximum security investment levels should never exceed 37% of the expected loss resulting from a security incident. While this seminal article spurred additional research pertaining to security investment decisions, use of the model depends on several parameters that are extremely difficult (if not impossible) to accurately calculate and/or estimate. Additionally, to use the model, a system's level of vulnerability must be subjectively determined as no metrics currently exist to objectively measure this construct. Accordingly, these limitations restrict practical application of the model.

Cavusoglu et al. (2004a) noted that increased network interconnectivity has elevated IS security concerns in most organizations, not just those that compete in high risk industries. Accordingly, they discuss several key factors that should be considered when determining the security investment level for an organization. The first factor they discuss concerns the tendency to greatly underestimate the potential losses resulting from intrusions by focusing solely on the tangible, short-term

costs necessary to recover operationally from an incident. The authors argue that inclusion of long-term and intangible costs in such estimates helps prevent under-investment in preventive measures. The second factor the authors discuss concerns the effectiveness of three commonly used strategies for evaluating investment alternatives. The first such strategy is based on practitioners' fears, uncertainty, and doubts (FUD) relating to security. The FUD strategy relies on the possibility of negative consequences to justify security investment. FUD has been widely used and loses strength after repeated usage. The second strategy is based on the cost of purchasing and deploying security technologies. This approach seeks to identify the amount of security coverage that can be purchased for a given amount of money. The weakness of this approach is that it does not attempt to balance investments and generated benefits. The third and final decision strategy focuses on computing the expected utility of each alternative to identify the options which offer the greatest benefits. Cavusoglu et al. (2004a) argue that this strategy yields the highest quality investment decisions.

Later in 2004, Cavusoglu et al. (2004b) proposed a game theory based model for evaluating the effectiveness IT security architectures. The authors note that many firms utilize a layered security architecture in which tiers of security controls are implemented that are both complementary and redundant. Accordingly, they argue that a layered decision model more accurately reflects the total utility provided by layered security architectures. Use of the model requires estimation of many hacker specific and firm specific parameters. These parameters include values such as of the fraction of dishonest, legitimate users and the expected utility hackers derive from breaking into systems. Given these estimated values, the authors stated that practitioners can use the model to determine the value derived by adding additional controls to their existing security architecture. However, practical application of the model is limited due the sheer quantity and complexity of input variables that must be estimated, in addition to the challenge of accurately estimating many of them.

In 2008, Cavusoglu et al. used mathematical modeling to compare game-theoretic and decision-theoretic approaches to security investment decisions. They argue that game-theoretic models yield larger payoffs when modeling the dynamic, strategic relationships that exist between firms and hackers. The researchers tested both models using the same sets of input parameters. Results showed that when the outcomes of the models were compared on the dimensions of investment level, vulnerability, and payoff, the game-theoretic model yields the highest payoff when the hacker and firm participate in a sequential game with the firm making the first move of the game. While these results add credence to the superiority of game-theory as a tool to model security investment decisions, practical implementation of the approach is again limited by the model's complexity and the larger number input parameters that must be accurately estimated with insufficient supporting data.

Wang et al. (2008) proposed incorporating extreme value analysis with the concept of value-at-risk to estimate daily losses due to critical security incidents. Extreme value analysis is a statistical method used to estimate maximum values in common probability distributions. Value at risk refers to probabilistic estimations of the maximum potential loss that could occur in a given situation. Using snapshots of data from a large financial institution, the authors simulate potential daily losses due to extreme security exploits. The researchers argue that this approach allows firms to appreciate the impact of critical IS security failures and choose the investment level that best represents their risk preference. As with previous studies, generalization of their results is limited by issues with estimating and/or calculating input parameters and the complexity of the model. Further, the study does not aid practitioners in quantifying the proportion of potential losses that should be spent to protect against such a loss.

All of these works add to the normative body of knowledge surrounding identification of an optimal security investment level assuming that all cost, benefits, and probabilities have been accurately estimated and a rational decision process is followed. These studies do not, however, add to our understanding of how practitioners currently make security investment decisions, nor do they explain those decisions. Further research is needed to guide quantitative estimation processes and to protect against any cognitive processes that could bias against rational behavior. A great deal of empirical evidence exists that demonstrates that humans do not always make rational decisions when faced with risk related decisions (Allais 1953; Crozier and Ranyard 1997; Kahneman and Tversky 1979; Slovic et al. 1977; Tversky and Kahneman 1981; Tversky and Kahneman 1992). Due to this, we feel that successful implementation of any of the above described methods first requires a deeper understanding of the cognitive processes used by practitioners when making security investment decisions.

Decision Theory

Decision Theory consists of a broad range of concepts and techniques used to describe and explain human decision making behavior. Within decision theory literature, three unique perspectives of decision related research exist (Edwards et al. 2007). The normative perspective of decision theory focuses on the use of logic and mathematics to determine the optimal option among several alternatives. All normative theories are characterized by basic assumptions concerning behavior in

choice situations. The dominant normative model is the expected utility model which views the decision process as consisting of two phases. In the first phase, the decision maker calculates the expected utility that could be realized by each decision option. In the second phase, the decision maker compares the expected utility of each option and selects the option that yields the greatest utility. Normative models are powerful tools for rationally comparing options to identify the superior option.

Models developed under the descriptive perspective of decision theory focus on the motives, cognitive processes, and mental models used by individuals to make decisions rather than on identifying the optimal option (Edwards et al. 2007). Descriptive models are thus focused on what humans actually do, rather than what they should do. Of the descriptive models of decision theory, Kahneman and Tversky's prospect theory is by far the most influential and utilized (Crozier and Ranyard 1997).

The last decision theory perspective is the prescriptive approach, which focuses on helping individuals make better decisions by using normative models with an awareness of the underlying motives, processes, and mental models that might influence their ability to make rational choices (Edwards et al. 2007). The interrelationship that exists between these three perspectives is depicted in Figure 1.

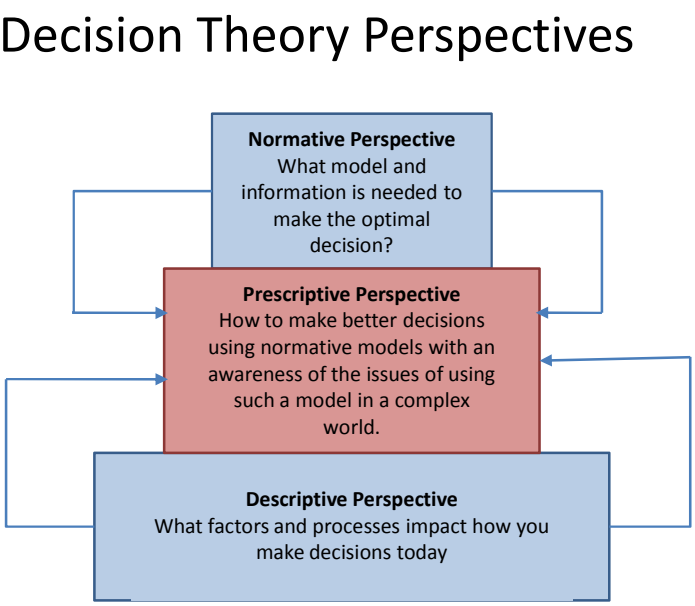

Figure 1 – Decision Theory Perspectives
Adapted from (Edwards et al. 2007)

Prospect Theory

Normative decision theories have a long history dating back to the eighteenth century, cumulating with publication of the expected utility model in 1947 (Miles Jr. 2007). Since then, expected utility has been used to analyze decision behavior in a variety of disciplines (Church et al. 2008; Devers et al. 2008; Edwards et al. 2007; Kahneman and Tversky 1979; Kumar, Park and Subramaniam 2008; Latham and Braun 2009; Tversky and Kahneman 1981; Tversky and Kahneman 1992; Wagner et al. 2009). However, French economist Maurice Allais (1953) noted inconsistencies between the choices predicted by the expected utility model and the actual choices made by individuals when faced with risk related decisions. Additionally, Herbert Simon (1957) observed that rationality in human decision making is bounded, due to limitations in time, information or cognitive resource. In work that provides great insight into why human decision making deviates from normative models, Kahneman and Tversky completed a series of studies documenting human behavior when faced with hypothetical risk related decisions (Kahneman and Tversky 1979; Tversky and Kahneman 1981; Tversky and Kahneman 1992).

In their first study (Kahneman and Tversky 1979), the researchers presented students and faculty at three universities with questionnaires containing hypothetical choice problems with clearly stated probabilities. Results showed that

respondents systematically violated the underlying principles of expected utility theory in three key ways. First, subjects tended to prefer certain outcomes to probabilistic outcomes even when the utility of the probabilistic option was greater than the utility of the certain outcome. Second, subjects disregarded components shared by all options and only evaluated the non-similar components of options. Finally, decision makers reversed their preferences when the framing of the decision was switched from a positive outcome to a negative outcome and vice-versa.

In a follow-up study, Tversky and Kahneman (1981) focused their efforts on understanding the effects of option framing on risk related decision preferences. For that study, participants read a short vignette describing the spread of a deadly Asian disease. Respondents were then presented with two hypothetical programs to combat the disease and asked to indicate which of two options they preferred. One half of the participants were presented with program options that were positively framed (i.e. lives saved), while the other half were presented with program options that were negatively framed (i.e. lives lost). An important element of the study was that all option pairs yielded the exact same level of utility when evaluated according to the principles of the expected utility models (200 people saved and 400 people die). Accordingly, if respondents evaluated the options in a rational manner, they should not exhibit a preference for any one of the two options. Similarly, there should be no significant difference in the response patterns to the positively and negatively framed options. Table 1 provides the scenario vignette and the positively and negatively framed option pairs that were used in the study.

Vignette: Imagine that the U.S. is preparing for the outbreak of an unusual Asian disease, which is expected to kill 600 people. Two alternative programs to combat the disease have been proposed. Assume that the exact scientific estimates of the consequences of the programs are as follows:	
Positively Framed Options:	**Negatively Framed Options:**
Program A: 200 people will be saved.	**Program C:** 400 people will die.
Program B: There is a 1/3 probability that 600 people will be saved, and a 2/3 probability that no people will be saved.	**Program D**: There is a 1/3 probability that nobody will die, and a 2/3 probability that 600 people will die.

Table 1. Classic Prospect Theory Vignette and Framed Options Adapted from Tversky and Khaneman (1981)

Results of the study showed that 72% of respondents who were presented with the positively framed options, preferred program A over program B, while 78% of respondents who were presented with the negatively framed options, preferred program D over program C (Tversky and Kahneman 1981). Thus, when respondents were faced with two positively framed options of equal utility, they preferred the more risk-averse option. Saving 200 lives was perceived as more desirable than the 1/3 probability of saving 600 lives coupled with the 2/3 probability of saving no lives. However, when faced with negatively framed options, respondents exhibited a different risk posture; respondents were risk-seeking, preferring the riskier of the two options. The 1/3 probability that no one die coupled with the 2/3 probability that all 600 people die was perceived as more desirable than the certainty of 400 people dying. Based on these results, Tversky and Khaneman concluded that decision behavior for risk related choices deviates significantly from expected utility.

Study Hypotheses

Based on Khaneman and Tversky's studies, we question whether framing of information security investment options influences, and therefore helps explain practitioner investment decisions. When proposing security investment options, practitioners have the option to discuss the investment in terms of the assets that will be protected with the investment (positive, or "gain" frame), or in terms of the assets that will be lost without the investment (negative, or "loss" frame). According to expected utility theory, such framing should have no impact on decision makers' preferences for investment options of equal utility. However, as information security investments are risk related decisions and the probabilities and outcome estimates used in such decisions are generally regarded as best-guesses, we believe that practitioners exhibit non-rational tendencies when making such decisions. Shropshire et al. (2010) found support for the notion that message framing influences security adoption behaviors. Accordingly, we put forth the following two hypotheses:

H1 When presented with two positively framed information security investment options of equal utility, security practitioners will prefer the more certain option.

H2 When presented with two negatively framed information security investment options of equal utility, security practitioners will prefer the less certain option.

METHODS

Instrument

To test our hypotheses, we developed an on-line survey instrument to assess practitioners' preferences pertaining to security investment options. Following the example of Tversky and Khaneman (1981), the instrument displays a short vignette, lists two investment options, and then asks respondents to indicate which of the two options they prefer. The vignette was worded to closely match the one used in Tversky and Khaneman's classic study. Each respondent is randomly presented either the negatively or positively framed investment options. Further, the order of investment options within each of these frames is randomized to eliminate the possibility of ordering bias; the less certain option is presented first for approximately one half of the respondents and presented last for the other half of the respondents. All presented investment options are of equal utility. Table 2 presents the vignette, the positively framed options, and the negatively framed options that were included in the on-line survey instrument.

Vignette: Imagine that your company is allocating financial resources to its information security program. Without such investment your company is expected to experience a $600,000 financial impact (asset loss). Note: Your assets include financial resources, intellectual property, organizational reputation, personnel time, and the confidentiality, integrity, and availability of your hardware, software, and data.	
Positively Framed Options:	**Negatively Framed Options:**
Program A: $200,000 worth of assets will be saved with certainty.	**Program A:** $400,000 work of assets will be lost with certainty.
Program B: There is a one-third probability that $600,000 worth of assets will be saved, and a two-thirds probability that no assets will be saved.	**Program B:** There is a one-third probability that no assets will be lost, and a two-thirds probability that $600,000 worth of assets will be lost.

Table 2. Information Security Investment Vignette and Framed Options

Sample

The target population for the study is individuals who have determined, or influenced the amount budgeted for information security at the organizational level. Such individuals may be at a variety of organizational levels, depending on the organization. We are sending personal invitations to participate to 100+ professional contacts of the study authors. We are also inviting local business leaders who participated in local area business training programs related to information security. Last, we are sending personal invitations to individuals who have shown an interest in the topic in various professional organizations, networking venues. Mass email invites are going out to a local InfraGard chapter (http://www.infragard.net) in a large, metropolitan city in the southwest, as well as information security professionals within the United States Department of Defense Information Assurance Technology Analysis Center (IATAC, http://iac.dtic.mil/iatac) Subject Matter Expert Program. A large percentage of InfraGard members and IATAC SMEs represent non-government organizations, while a smaller percentage are U.S. government employees.

To ensure that all survey respondents are actual members of the target population, the first question that is presented following the informed consent release asks respondents, "Have you determined the amount, or influenced the decision, of how much money is budgeted for information security at an organizational level?" Respondents who reply *yes* to this question are prompted to enter the number years of experience they have influencing or determining such decisions and are then are presented with the vignette and the framed investment options. Respondents who reply *no* to the above question, are thanked for their interested in the investigation and then exited from the questionnaire.

Data Analysis Method

Collection of data to test our stated hypothesis is currently underway. Once a large enough sample of responses has been collected, the responses will be analyzed using the Chi Squared Independence Test. This test is used to assess the

degree of association between two categorical variables and is the test statistic that was used by Kahneman and Tversky to analyze their data. The test will show if there is a significant difference in the respondents' preferences for more or less certainty regarding information security investments, due to the framing of the question.

Closing Remarks

The results from this research will show whether information security investment decision makers are rational or not, and whether their decisions are influenced by classic prospect theory framing effects. The academic contribution is greater understanding of the investment decision process regarding information security, which will support future modeling and decision aid research. The practical contribution to the lower level IT practitioner is evidence that framing does matter, suggesting whether it is worthwhile for budget justifications to be framed positively versus negatively. The longer-term practical contribution is the development of prescriptive models for such decision making.

Development of normative decision models is an imperative component of efforts to assist practitioners with making better information security investment decisions. However, before normative models can be positioned as prescriptive aids to guide decision makers, we must first develop a clear understanding of how information security investment decisions are made today. This includes developing a thorough understanding of the real-world decision heuristics that are employed, which may bias decision makers against rational evaluation of investment options. This study adds to the normative decision model line of research by demonstrating the effects of framing on information security investment options.

REFERENCES AND CITATIONS

1. Allais, P.M. (1953), "Le Comportement De L'Homme Rationnel Devant Le Risque: Critique Des Postulats Et Axiomes De L'Ecole Americaine," *Econometrica* (21:4), October 1953 pp 503-546.
2. Cavusoglu, H., Cavusoglu, H., and Raghunathan, S. (2004a), "Economis of IT Security Management: Four Improvements to Current Security Practices," *Communications of AIS* (14) pp 65-75.
3. Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004b), "A Model for Evaluating IT Security Investments," *Communications of the ACM* (47:7) pp 87-92.
4. Cavusoglu, H., Raghunathan, S., and Yue, W.T. (2008), "Decision-Theoretic and Game-Theoretic Approaches to IT Security Investments," *Journal of Management Information Systems* (25:2) pp 281-304.
5. Church, B.K., Libby, T., and Ping, Z. (2008), "Contracting Frame and Individual Behavior: Experimental Evidence," *Journal of Management Accounting Research* (20) pp 153-168.
6. Computing Researcher Association (2006) "Four Grand Challenges in Trustworthy Computing," in: *Second Confternece on Grand Challenges in Computer Science and Engineering*, Warrenton, VA.
7. Crozier, W.R., and Ranyard, R. (1997) "Cognitive process models and explanations of decision making," in: *Decision making: cognitive models and explanations,* R. Ranyard, W.R. Crozier and O. Svenson (eds.), Routledget, New York, pp. 5-20.
8. Devers, C.E., McNamara, G., Wiseman, R.M., and Arrfelt, M. (2008), "Moving closer to the action: examining compensation design effects on firm risk," *Organization Science* (19:4) pp 548-566.
9. Edwards, W., Miles Jr., R.F., and Von Winterfeld, D.V. (2007) "Introduction: Advances in decision analysis from foundations to applications," in: *Advances in decision analysis from foundations to applications,* W. Edwards, R.F. Miles Jr. and D.V. Winterfled (eds.), Cambridget University Press, New York pp. 1-12.
10. Gal-Or, E., and Ghose, A. (2005), "The Economic Incentives for Sharing Security Information," *Information Systems Research* (16:2) pp 186-208.
11. Gordon, L.A., and Loeb, M.P. (2002), "The Economics of Information Security Investment," *ACM Transactions on Information and Systems Security* (5:4) p 438.
12. Herath, H.S.B., and Herath, T.C. (2008), "Investments in Information Security: A Real Options Perspective with Bayesian Postaudit," *Journal of Management Information Systems* (23:3) pp 337-375.
13. Kahneman, D., and Tversky, A. (1979), "Prospect Theory: An Analysis of Decision under Risk," *Econometrica* (47:2) pp 263-291.
14. Latham, S.F., and Braun, M. (2009), "Managerial Risk, Innovation, and Organizational Decline," *Journal of Management* (35:2) pp 258-281.
15. Shropshire, J.D., Warkentin, M., and Johnston, A.C. (2010), "IMPACT OF NEGATIVE MESSAGE FRAMING ON SECURITY ADOPTION," *The Journal of Computer Information Systems* (51:1) pp 41-51.
16. Slovic, P., Fischhoff, B., and Lichtenstein, S. (1977), "Behavior Decision Theory," *Annual Review of Psychology* (28) pp 1-39.
17. Tversky, A., and Kahneman, D. (1981), "The Framing of Decisions and the Psychology of Choice," *Science* (211) pp 453-458.
18. Tversky, A., and Kahneman, D. (1992), "Advances in prospect theory: Cumumlative representation of uncertainty," *Journal of Risk and Uncertainty* (5), November 1992 pp 297-323.
19. U.S. Department of Homeland Security (2009) "A Roadmap for Cybersecurity Research," H. Security (ed.).
20. Wagner, T., Hennig-Thurau, T., and Rudolph, T. (2009), "Does Customer Demotion Jeopardize Loyalty?," *Journal of Marketing* (73:3) pp 69-85.
21. Wang, J., Chaudhury, A., and Rao, H.R. (2008), "A Value-At-Risk Approach to Information Security Investment," *Information Systems Research* (19:1) pp 106-120.
22. West, R. (2008), "The Psychology of Security," *Communications of the ACM* (51:4) pp 34-40.
23. Zafar, H., and Clark, J.G. (2009), "Current State of Information Security Research in IS," *Communications of AIS* (24), June 2009 pp 557-596.
24.